UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/034,485	12/28/2001	Jong-Uk Choi	30360/37968	2206

4743 7590 05/04/2006

MARSHALL, GERSTEIN & BORUN LLP
233 S. WACKER DRIVE, SUITE 6300
SEARS TOWER
CHICAGO, IL 60606

EXAMINER	
BAYAT, BRADLEY B	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 05/04/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/034,485	CHOI ET AL.	
	Examiner	Art Unit	
	Bradley B. Bayat	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 March 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *20-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *20-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on March 16, 2006 has been entered.

Status of Claims

This communication is in response to amendment filed on March 16, 2006

- Claims 1-19 have been canceled.
- New claims 20-37 have been added.

Response to Arguments

Applicant's arguments with respect to claims have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 20-37 are rejected under 35 U.S.C. 102(e) as being anticipated by US 2001/0016836 A1 to Boccon-Gibod et al.

As per the following claims, Boccon-Gibod et al. disclose:

20. (New) A digital information security system comprising:

a user application tool installed in a user terminal, the user application tool being structured to create a unique user key using unique system information of the user terminal, to transmit the unique user key to a server system via a network for registration and to subsequently transmit the unique user key to the server system via the network for authentication (figure 2, 130; software installed on client);

the server system comprising an encryption unit to encrypt digital information, a user information database to store the user information including the unique user key received from the user terminal for registration, a digital information database to store the encrypted digital information, a rule establishing unit to establish a rule corresponding to the user information and the digital information, a coupling unit to encrypt, using the unique user key, rule information corresponding to the rule, to encrypt, using the unique user key, a decryption key for decrypting the digital information, and to combine the encrypted rule information, the encrypted decryption key and the encrypted digital information into combined information, and a digital file database to store the combined information (figure 2, server 100); and

the server system also comprising a server control unit including a user management tool to perform a user authentication process by comparing the unique user key stored in the user information database with the unique user key subsequently transmitted from the user terminal for authentication (figure 2, 210, 220),

wherein the server control unit transmits the combined information from the digital file database to the user application tool after completing the user authentication process, when the user terminal requests a download of the digital information (fig 2, 200-240).

21. (New) The digital information security system as claimed in claim 20, wherein when the combined information is downloaded to the user application tool, it is determined whether the digital file should be decrypted by determining whether the key used for encrypting the decryption key matches the unique user key created by the user application tool [¶0008-0012, 0039-0042].

22. (New) The digital information security system as claimed in claim 20, wherein the rule establishing unit establishes a rule for one or more of authority of storage, authority of print, authority of allowable time for use; and authority of transfer of the digital file [0036-0038].

23. (New) The digital information security system as claimed in claim 20, wherein the system information includes wherein the unique system information includes at least one of unique CPU (Central Processing Unit) information, unique HDD (Hard Disk Drive) information, and serial number information of the user terminal [0008-0009, 0032-0034, 0041-0043].

24. (New) A digital information security method comprising the steps of:

creating a unique user key using unique system information of a user terminal using a user application tool installed in a user terminal (fig 4, 400-440)

transmitting digital information and user information including the unique user key from the user terminal to a server system via a network ((fig 4, 450-460, fig 5, 500);

encrypting the digital information and the user information including the unique user key transmitted from the user terminal (fig 5);

storing the encrypted user information and the encrypted digital information in the server system (fig 5);

establishing a rule corresponding to the user information and the digital information (fig 5-6 and associated text);

encrypting the rule and a decryption key for decrypting the digital information using the unique user key(fig 5-6 and associated text);

combining the encrypted digital information, the encrypted rule and the encrypted decryption key into combined information(fig 5-6 and associated text);

storing the combined information (fig 5-6 and associated text);

performing a user authentication process by comparing the unique user key stored in the server with the unique user key subsequently transmitted from the user application tool of the user terminal for authentication(fig 5-6 and associated text);

transmitting the combined information from the server system to the user application tool via the network after completing the user authentication process, when the user terminal requests a download of the digital information (fig 5-6 and associated text); and

determining, with the user application tool, whether the digital file should be decrypted by determining whether the key used for encrypting the decryption key matches the unique user key created by the user application tool (fig 5-6 and associated text).

25. (New) The digital information security method as claimed in claim 24, wherein the rule includes one or more of authority of storage, authority of print, authority of allowable time for use, and authority of transfer of the digital information [see claim 22].

26. (New) The digital information security method as claimed in claim 24, wherein the unique system information includes at least one of unique CPU (Central Processing Unit) information, unique HDD (Hard Disk Drive) information, and serial number information of the user terminal [see claim 23].

27. (New) A digital information encryption and upload method comprising the steps of

creating a unique user key using unique system information of a user terminal using a user application tool installed in a user terminal;

uploading digital information, user information including the unique user key from the user terminal to a server system;

encrypting the digital information and the user information including the unique user key transmitted from the user terminal;

storing the encrypted user information and the encrypted digital information in the server system;

establishing a rule corresponding to the user information and the digital information;

encrypting the Me and a decryption key for decrypting the digital information using the unique user key;

combining the encrypted decryption key, the encrypted digital information, and the encrypted rule into a combined file; and

storing the combined file.

28. (New) The digital information encryption and upload method as claimed in claim 27, wherein the rule includes one or more of authority of storage, authority of print, authority of allowable time for use, and authority of transfer of the digital information..

29. (New) The digital information encryption and upload method as claimed in claim 27, wherein the unique system information includes at least one of unique CPU (Central Processing Unit) information, unique HDD (Hard Disk Drive) information, and serial number information of the user terminal.

30. (New) An encrypted digital information download method comprising the steps of.

creating a unique user key using unique system information of a user terminal using a user application tool installed in a user terminal;

transmitting a request from the user terminal to a server system to download digital information from the server system;

transmitting the unique user key from the user terminal to the server system;

performing a user authentication process at the server system by comparing a unique user key stored in the server system with the unique user key transmitted from the user terminal;

transmitting a digital file from the server to the user terminal when the user terminal is authenticated, the digital file including an encrypted version of the digital information and an encrypted decryption key, the decryption key for decrypting the encrypted version of the digital information; and

decrypting, at the user terminal, the encrypted version of the digital information if the key used for encrypting the decryption key matches the unique user key created by the user application tool,

31. (New) The digital information download method as claimed in claim 30, further comprising:

establishing a rule associated with the digital information, wherein the rule includes one or more of authority of storage, authority of print, authority of allowable time for use, and authority of transfer of the digital information;

wherein the digital file includes an encrypted version of the rule.

32. (New) The digital information download method as claimed in claim 30, wherein the unique system information includes at least one of unique CPU (Central Processing Unit) information, unique HDD (Hard Disk Drive) information, and serial number information of the user terminal.

33. (New) A digital information security method in a system in which a digital information server and a plurality of user systems are connected via a network,

receiving, at the digital information server, a download request from one user system of the plurality of user systems, the download request for digital information;

combining into a file an encrypted version of the digital information, a decryption key for decrypting the encrypted version of the digital information, and a rule corresponding to the digital information, wherein the rule corresponding to the digital information includes authority of use of the digital information and includes authority of transfer indicating whether the one user system can transfer the digital information to another user system;

transmitting the file from the digital information server to the one user system in response to the download request;

decrypting at the one user system the encrypted version of the digital information by the use of the decryption key; and

utilizing at the one user system the digital information in accordance with the rule corresponding to the digital information, and

transferring the digital information from the one user system to another user system in accordance with the rule corresponding to the digital information.

34. (New) The digital information security method as claimed in claim 33, further comprising:

setting, using the digital information server, a plurality of groups, each group including a plurality of user systems; and

establishing, using the digital information server, a plurality of rules, each rule of the plurality of rules corresponding to each group;

wherein the one user system is in one of the groups, wherein the rule corresponding to the digital information includes the rule corresponding to the group;.

35. (New) The digital information security method as claimed in claim 33, wherein the decryption key in the file and the rule corresponding to the group in the file are encrypted.

36. (New) The digital information security method as claimed in claim 35, wherein the decryption key in the file and the rule corresponding to the group in the file may be decrypted using a unique user key created using unique system information of the one user system.

37. (New) the digital information security method as claimed in claim 36, wherein the unique system information includes at least one of unique CPU (Central Processing Unit)

information, unique HDD (Hard Disk Drive) information, and serial number information of the one user system.

Claims 27-37 are directed to subject matter similar to rejected claims 20-26. Claims 27-37 are therefore rejected accordingly.

Although the Examiner has pointed out particular references contained in the prior art(s) of record in the body of this action, the specified citations are merely representative of the teachings in the art as applied to the specific limitations within the individual claim. Since other passages and figures may apply to the claimed invention as well, it is respectfully requested that the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- US 2002/0107809 A1 to Biddle et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Bradley B. Bayat whose telephone number is 571-272-6704. The examiner can normally be reached on Tuesday - Friday 8 a.m.-6:30 p.m. and by email: bradley.bayat@uspto.gov. If attempts to reach the examiner by telephone are unsuccessful, the

examiner's supervisor, James Trammell can be reached regarding urgent matters at 571-272-6712.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

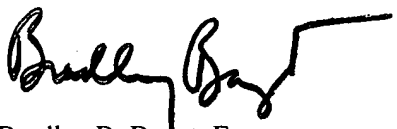
Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, D.C. 20231

Or faxed to:

(571) 273-8300 - Official communications; including After Final responses.

(571) 273-6704 - Informal/Draft communications to the examiner.



Bradley B. Bayat, Esq.
Department of Commerce - USPTO
KNOX - 5A48
Technology Center 3600
Art Unit 3621 - Patent Examiner
(571) 272-6704 Direct Dial
(571) 273-6704 Direct Fax
(571) 273-8300 Official Central Fax